UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
08/989,261	12/12/97	PAONE L	831-2

WM51/1030

CHARLES R HOFFMANN
HOFFMANN & BARON LLP
6900 JERICHO TURNPIKE
SYOSSET NY 11791

EXAMINER	
KABAKOFF,S	
ART UNIT	**PAPER NUMBER**
2132	10

DATE MAILED: 10/30/00

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

Office Action Summary	Application No.	Applicant(s)	
	08/989,261	PAONE, LUCIANO F.	
	Examiner	Art Unit	
	Steve Kabakoff	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136 (a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).

Status

1)☒ Responsive to communication(s) filed on *30 August 2000* .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,5-24,30-32,34 and 36-40* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,11,17,19,20,30-32 and 34* is/are rejected.

7)☒ Claim(s) *5-10,12-16,18,21-24 and 36-40* is/are objected to.

8)☐ Claims _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are objected to by the Examiner.

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

a)☐ All b)☐ Some * c)☐ None of the CERTIFIED copies of the priority documents have been:

1.☐ received.

2.☐ received in Application No. (Series Code / Serial Number) _____ .

3.☐ received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. & 119(e).

Attachment(s)

15) ☒ Notice of References Cited (PTO-892)
16) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
17) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
18) ☒ Interview Summary (PTO-413) Paper No(s). *8* .
19) ☐ Notice of Informal Patent Application (PTO-152)
20) ☐ Other: .

DETAILED ACTION

1. Claims 1, 2, 5-24, 30-32, 34, and 36-40 have been examined.

2. The applicant amended claims 1, 2, 5, 7, 8, 9, 21, and 22.

The applicant canceled claims 3, 4, 25-29, 33, and 35.

The applicant added new claims 36-40.

Response to Arguments

3. The objections to claim 21 have been removed in light of the amendments made in the applicant's response received August 30, 2000 (paper number 9).

4. Applicant's arguments with respect to claims 1-24, 30-32, and 34 have been considered but are moot in view of the new ground(s) of rejection.

The amendments made to the claims and the applicant's corresponding explanation of a "dynamic key schedule" presented in the applicant's response filed August 30, 2000 (paper number 9), and the applicant's description of "modifying the key schedule based upon the modified object key" discussed in a telephone interview on August 7, 2000 (paper number 8) obviated the Examiner's claim rejections using Wood (US 5003596). The dynamic key schedule, as defined by the applicant's correspondences and claim amendments, is in contrast to the static key schedule used in Wood (US 5003596). As the applicant attests on page 16 of his reply filed August 30, 2000: "it is the 'dynamic', i.e., changing object key with each block of input data and the corresponding 'dynamic' key schedule based upon the dynamic object key which is the essence of the invention."

Moreau (US 6069954) teaches a key schedule comprising a plurality of linear feedback shift registers (LFSR); each LFSR generates a pseudo-random key sequence used to encrypt a unique block of cleartext data. A linear feedback shift register inherently modifies itself via a feedback mechanism such that the value of a LFSR at time t+1 is a function of the previous value of the same LFSR at time t. Furthermore, each LFSR inherently must be set to an initial state.

Therefore, the key schedule in Moreau (US 6069954) is dynamically modified based on at least one modified LFSR. Similarly, a key schedule in the claimed inventions is dynamically modified based on at least one modified object key. Thus the at least one LFSR in Moreau (US 6069954) is equivalent to the at least one object key in the claimed inventions.

For those claims that remain rejected, the Examiner will again rely on Colvin, Sr (US 5841872) as evidence it would have been obvious to one of ordinary skill in the art at the time of the invention to implement the LFSRs in Moreau (US 6069954) using object-oriented programming.

Claim Objections

5. Claims 37-40 are objected to because of the following informalities:

The word "tanspositioning" should be changed to "transpositioning" in line 27 of claim 37.

The word "bonded" should be changed to "bounded" in line 29 of claim 37.

Appropriate correction is required.

6. Claim 34 is objected to because of the following informalities:

The phrase "provides a **coat** of substitution rounds" in line 3 of claim 34 appears to contain a typographical error.

Allowable Subject Matter

7. Claims 5-10, 12-16, 18, 21-24, and 36-40 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

As per claim 5, the claimed invention limits claim 1 so the following is done before the step of encrypting:

(i) the user creates an initial state of the at least one object key

(ii) an initial state of a random session key is created

(iii) the initial state of the random session key is encrypted using the initial state of the at least one object key

(iv) the object key is modified based on seeding from the random session key before each input data block is encrypted to ensure each input data block is encrypted using a unique key

Step (i) is standard in OOP when an object's constructor is executed (in Colvin, Sr (US 5841872), the constructor is DataSpin::DataSpin). The method of Colvin, Sr (US 5841872) shows a typical constructor that initializes an encryption key (the eight state variables in class DataSpin) which would be used to initialize a linear feedback shift register (LFSR) object in Moreau (US 6069954).

Step (ii) is inherent in Moreau (US 6069954) since a random initializing vector is created to seed the LFSRs that comprise the key schedule (see Fig. 2).

Step (iii) discloses encrypting the initial state of the random initializing vector (R_o) with the initial state of the at least one object key (K_o). Step (iv) discloses modifying at least one object key at time t (K_t) based on seeding from the random session key at time t (R_t). Therefore,

steps (iii) and (iv) in claim 5 teach two separate objects: an object key and a random session object, that interact as taught in steps (iii) and (iv) respectively.

In the closest pieces of prior art found by the Examiner, Moreau (US 6069954) and Colvin, Sr (US 5841872), a LFSR object at time t (K_t) is modified based on seeding from its own value at time t (K_t). Therefore, the prior art of record only discloses the limitations in steps (iii) and (iv) of claim 5 if the LFSR object and the random session object are the same (ie, only if $R_i = K_i$). However, as stated previously, claim 5 discloses the interaction of a separate object key and random session key, and therefore the prior art of record, neither alone nor in combination with other cited prior art references, teaches steps (iii) and (iv) in claim 5.

As per claims 6-8, and 12-16, and 18, the claimed inventions depend on independent claim 5 and therefore contain the same allowable subject matter.

As per claim 9, a method of modifying an object key is disclosed comprising specific rotations, multiplications, transpositions, and additions that are repeated for a fixed number of times. Although each step in the key modification is known separately, the examiner was not able to find in a single reference or a combination of references the specific sequence of operations disclosed in claim 9.

As per claims 36-40, the claimed inventions contain the same allowable subject matter as claim 9.

As per claim 10, the claimed invention limits claim 1 so the object key is dynamic and modification of the object key uses a hashing function. The method disclosed by Moreau (US 6069954) and Colvin, Sr (US 5841872) teaches a dynamic LFSR object key, but the method of Moreau (US 6069954) and Colvin, Sr (US 5841872) does not teach modifying the key using a hashing function. Instead of using non-linear hashing functions, the cited prior art uses "linear

feedback," and consequently the prior art of record would not motivate one of ordinary skill in the art to use hashing functions in combination with LFSR objects.

As per claim 21, a method of block cipher encryption is disclosed comprising repeated substitutions using the output from a transpositioning transverse array whose elements contain unique numbers; the outputs are summed and rotated in a sliding window and modulo-2 added to an element of a key, then repeated substitutions using the transpositioning transverse array are applied again. A final scrambling step is performed at the end of each round of encryption, where a specific number of rounds is disclosed in the encryption method.

The examiner was not able to find in a single reference or a combination of references that teach the specific sequence of operations disclosed in claim 21.

As per claims 22-24, the claimed inventions depend on claim 21 and therefore contain the same allowable subject matter.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1, 2, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moreau (US 6069954) in view of Colvin, Sr (US 5841872).

As per claim 1, Moreau (US 6069954) teaches a block encryption method to convert a block of input cleartext into a unique block of ciphertext (see Fig. 2). In the method of Moreau (US 6069954), encryption keys are selected from a dynamic key schedule for use in the

encryption process (see the 10 LFSRs in Fig. 2). Since the key schedule in Moreau (US 6069954) comprises a plurality of LFSRs, the key schedule inherently modifies itself based on the modification of individual linear feedback shift registers. The block encryption method in Moreau (US 6069954) differs from the block encryption method in claim 1 since the encryption keys in Moreau (US 6069954) are not object keys as defined in claim 1.

The "object key comprising data and methods" in claim 1 is interpreted by the examiner to refer to an object associated with object-oriented programming (OOP). Anyone skilled in the art of computer science would know an *object* in OOP is composed of *data* (sometimes referred to as "attributes") and *methods*. Therefore, one skilled in the art would understand the object key in claim 1 to comprise methods designed to implement an encryption process and corresponding data to support the methods.

The examiner asserts that it is well known to implement encryption using OOP. In fact, encryption classes are ubiquitous in the art of programming in high level languages such as C++ and Java. It appears the examiner who wrote the first office action presented the Shanton (US 5369702) reference to illustrate an object-oriented encryption system, however Colvin, Sr (US 5841872) more explicitly shows a block encryption process implemented using an OOP encryption class.

In Colvin, Sr (US 5841872), column 4, lines 25-66 show a specific encryption class "DataSpin" comprising data (S, T, U, V, W, X, Y, and Z) and methods (SPIN_LEFT and SPIN_RIGHT). Column 5, lines 40-43 in Colvin, Sr (US 5841872) explain that the state variables in the disclosed encryption class are equivalent to an encryption key.

The applicant may assert the encryption key object in Colvin, Sr (US 5841872) does not implement the same block encryption method taught in the claimed inventions; this is correct. *The Colvin, Sr (US 5841872) reference is simply being used as evidence to show how an*

encryption key object containing data and methods, such as the object key in claim 1, is a very well known OOP encryption class implementation.

Therefore, one of ordinary skill in the art of programming would know to code the encryption keys in Moreau (US 6069954) using OOP to create an encryption key object similar to that in Colvin, Sr (US 5841872). It would have been obvious to one of ordinary skill in the art at the time of the invention to create the encryption key in Moreau (US 6069954) using OOP, as shown in Colvin, Sr (US 5841872), since OOP is well known in the art as a means for compact, modular, high-level coding of block encryption processes.

As per claim 2, the claimed invention limits claim 1 so the modification of the key schedule is independent of the input plaintext. The modification of the LFSR objects in the encryption process disclosed in Moreau (US 6069954) and Colvin, Sr (US 5841872) does not depend on the input cleartext (see Fig. 2).

As per claim 19, the claimed invention limits claim 2 so the encrypting step uses a substitution array where the transposition of elements in the array is dependent upon an element of a key. Put another way, claim 19 teaches a keyed substitution array in the encrypting step. The method of encrypting taught in Moreau (US 6069954) also uses a keyed substitution array in the "Decision Machine" in Figs. 1-3 (ie, see "Permutation Logic" keyed by the "Permutation ROM" in Figs. 2 and 3).

As per claim 30, the claimed invention contains the same limitations as previously rejected claim 1 and is rejected for the same reasons.

As per claims 31 and 32, the key schedule in Moreau (US 6069954) inherently comprises LFSRs that must be keyed to an initial state before they are clocked. Therefore, the initial vector input to the LFSRs is the same as the claimed "random session object key," where it would have been obvious to one of ordinary skill in the art at the time of the invention to

initialize the LFSR objects in the method of Moreau (US 6069954) and Colvin, Sr (US 5841872) using random numbers so the LFSR key objects can not easily be reproduced by someone trying to reverse engineer the dynamic key schedule in Moreau (US 6069954).

The Examiner notes that claims 31 and 32 differ from claim 5 since they do not disclose both steps (iii) and (iv) in claim 5 which in combination were identified as containing allowable subject matter.

As per claim 34, the claimed invention contains the same limitations as previously rejected claim 19 and is rejected for the same reasons.

10. Claims 11 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moreau (US 6069954) in view of Colvin, Sr (US 5841872) and in further view of official notice.

As per claim 11, the claimed invention limits claim 1 so the object key is dynamic and includes at least two sub-object keys each with its own modification method. The block encryption method disclosed by Moreau (US 6069954) and Colvin, Sr (US 5841872) does not explicitly teach using at least two sub-LFSR object keys each with its own modification method. Official notice is taken that a single LFSR can be broken into smaller LFSRs that together perform the same function as the single LFSR.

As per claim 20, the claimed invention limits claim 19 so the position provided by an element of the key is bounded by the size of the substitution array. As discussed in regards to claim 19, the method taught by Moreau (US 6069954) and Colvin, Sr (US 5841872) teaches a keyed substitution array, but does not bound the element position provided by the array by the size of the array itself. Official notice is taken that a large substitution array can provide a larger number of element positions than a small substitution array. In other words, a 2-by-2 substitution array will not be able to provide as many key positions as a 10-by-10 array, and

thus one would be motivated to use a larger substitution array since more possible key positions in a substitution array is harder to cryptanalyze.

11. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Moreau (US 6069954) in view of Colvin, Sr (US 5841872) and in further view of Campbell, Jr (US 4369332).

As per claim 17, the claimed invention limits claim 2 so the plaintext is padded to be divisible by the block length. The method taught by Moreau (US 6069954) and Colvin, Sr (US 5841872) fully discloses the limitations in claim 2, but does not teach padding (or salting) plaintext blocks to make them a fixed length.

The examiner notes this is common practice in the art of block encryption systems and the Campbell, Jr (US 4369332) reference is one of many references that teach the limitation in claim 17 (see column 4, lines 55-62 of Campbell, Jr (US 4369332)).

It would have been obvious to one of ordinary skill in the art at the time of the invention to pad plaintext blocks to make them a fixed length, as taught in Campbell, Jr (US 4369332), in the block encryption method taught by Moreau (US 6069954) and Colvin, Sr (US 5841872), since it is common practice in the art of block encryption systems to pad or salt plaintext blocks.

Conclusion

12. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Kaufman et al (US 5764772)

Shanton (US 5369702)

Kawano et al (US 5995623)

Takeshima (JP 09093242A)

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Steve Kabakoff whose telephone number is (703) 306-4153. The examiner can normally be reached on 8:30am to 6:00pm except every other Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tod Swann can be reached on (703) 308-7791. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 305-0040 for regular communications and (703) 305-9051 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

TOD R. SWANN
SUPERVISORY PATENT EXAMINER
GROUP 2700

10/25/00
SK